EXHIBIT F – 2-B

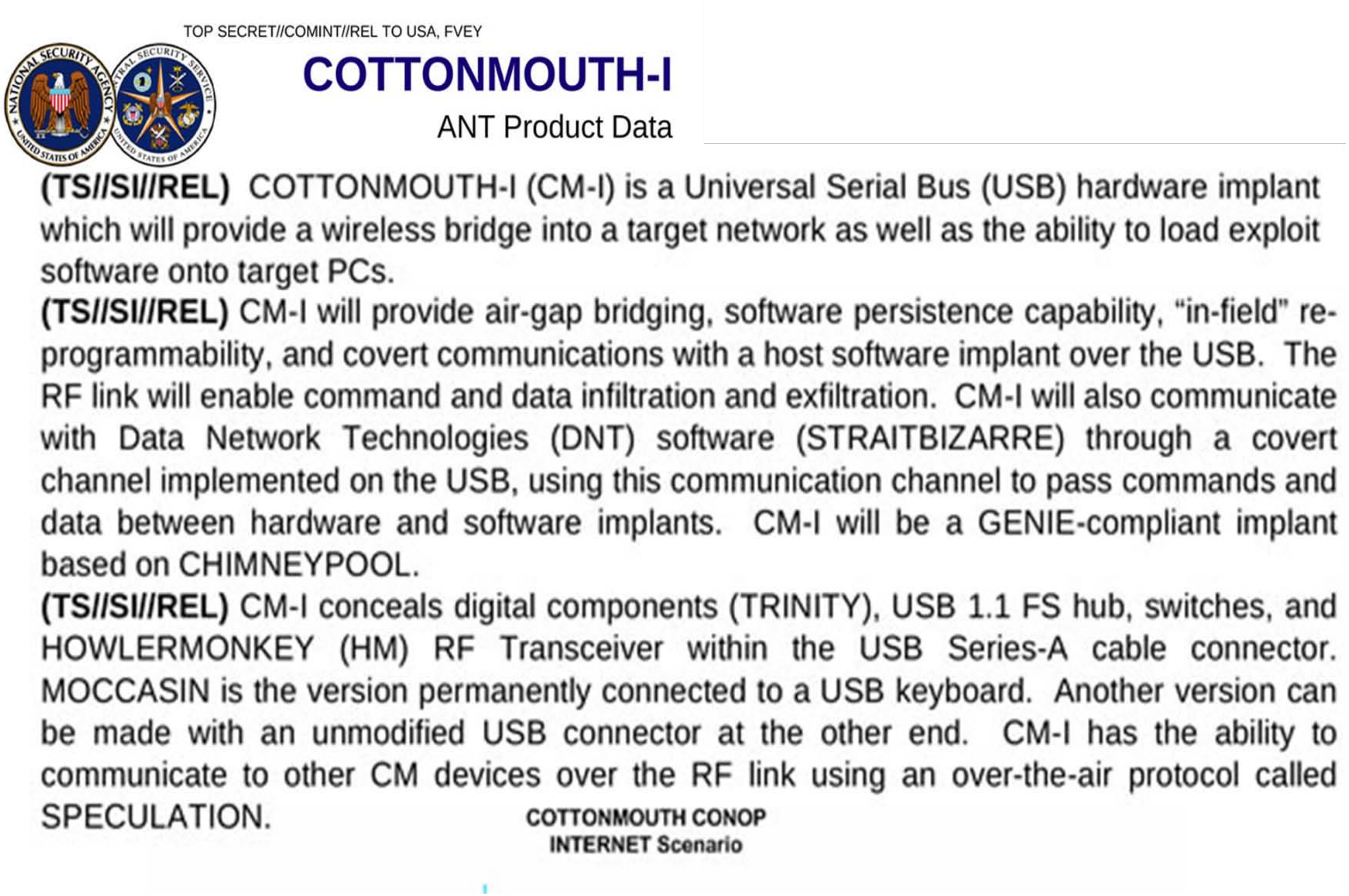
Exhibit 2: The National Security Agency (NSA): "NSA Playkit"

The National Security Agency (NSA) has constructed track and trace and other communications and signals intelligence, i.e., "comint" and "sigint" devices that must use plaintiff's microwire and/or plaintiff's radio frequency patents to achieve optimal performance. NSA is using these current generation devices for multiple classified uses, including cyber surveillance and submarine assisted deep sea monitoring of optical fiber communications cables, asset targeting, human asset tracking and monitoring and much more.

Exhibit 2. B. NSA Product Description: Universal Serial Busses (USB) for Covert Intelligence Gathering

An encoded microwire key is embedded into or onto a miniaturized chip (hardware implant) along with covert software that is inserted into USB devices. The microwire provides a radio frequency link that allows for infiltration and exfiltration of data. The computers or personal electronic devices to which encoded microwire USB keys are attached can be remotely controlled and monitored. The encoded microwire USB keys can also be used to track the location of the attendant device by ISP address at great distances and by microwave interrogation at even greater distances by satellites.

Government Infringement for USB Covert Intelligence Gathering



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

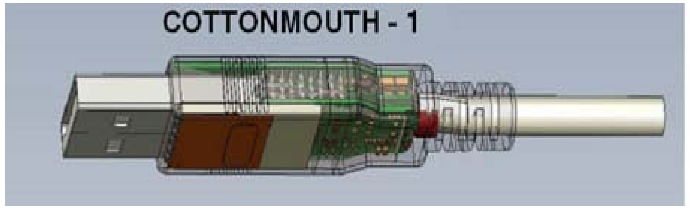
ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

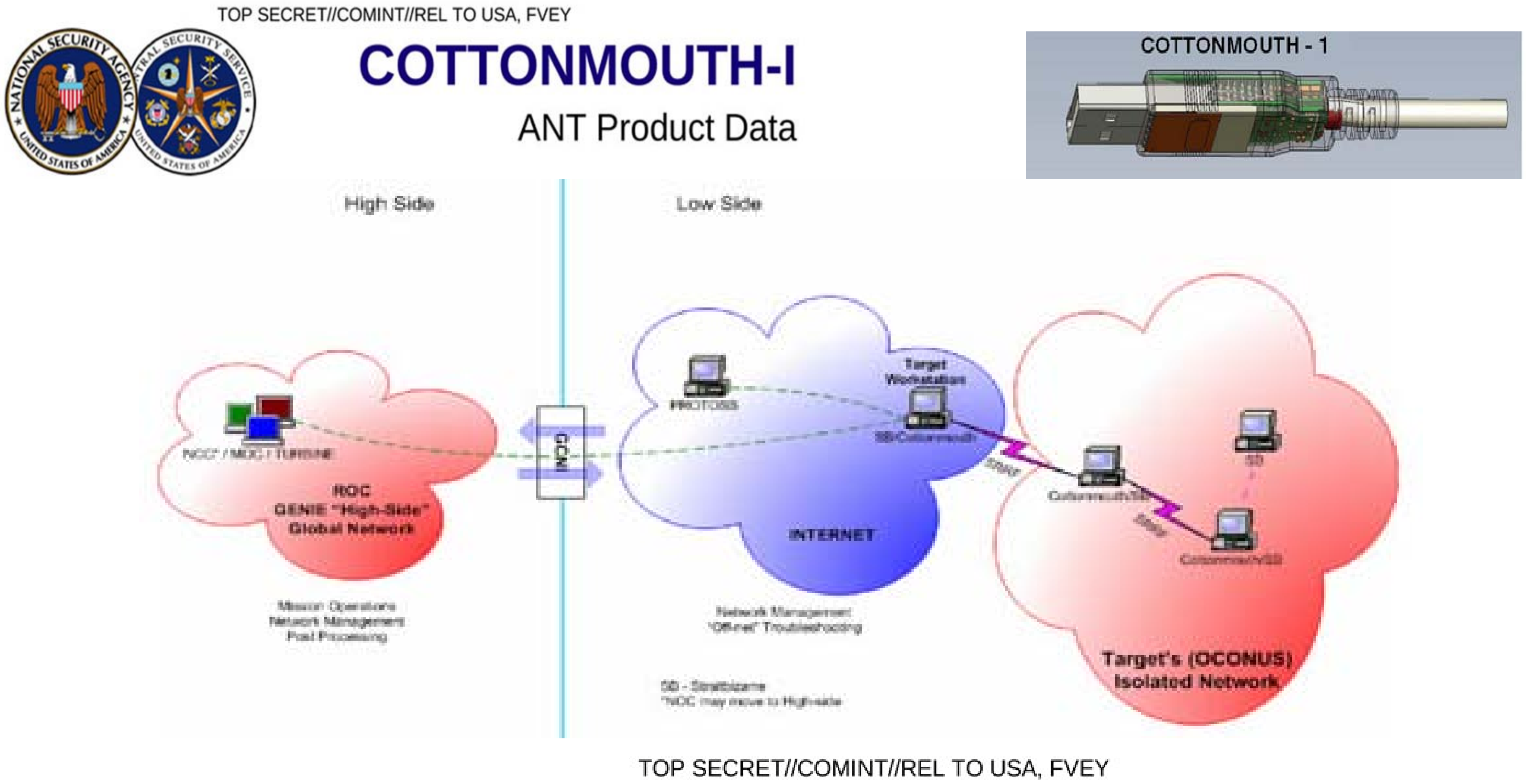
(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP
INTERNET Scenario



TOP SECRET//COMINT//REL TO USA, FVEY

Government Infringement for USB Covert Intelligence Gathering



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

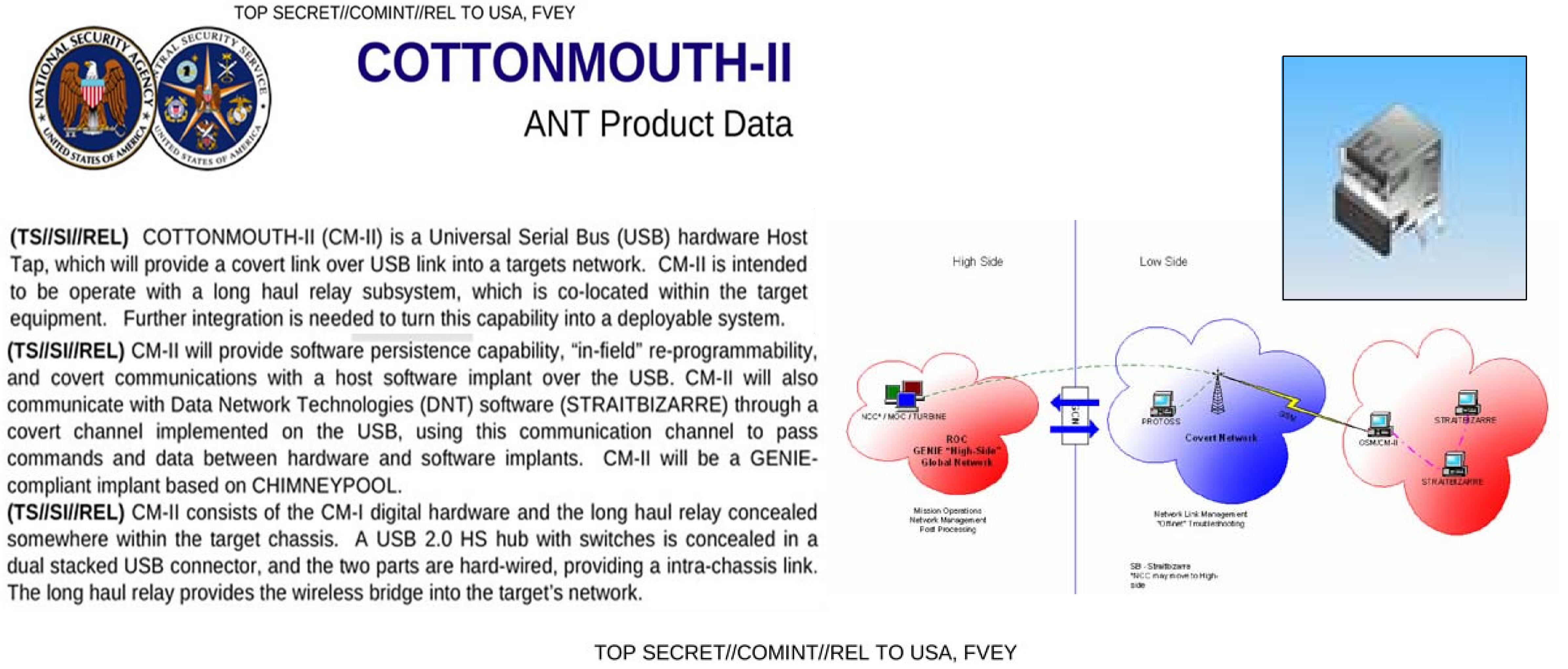
Mission Operations
Network Management
Post Processing

Network Management
"Off-net" Troubleshooting

SB - Straitbizarre
*NOC may move to High-side

TOP SECRET//COMINT//REL TO USA, FVEY

Government Infringement for USB Covert Intelligence Gathering



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-II

ANT Product Data

(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed to turn this capability into a deployable system.

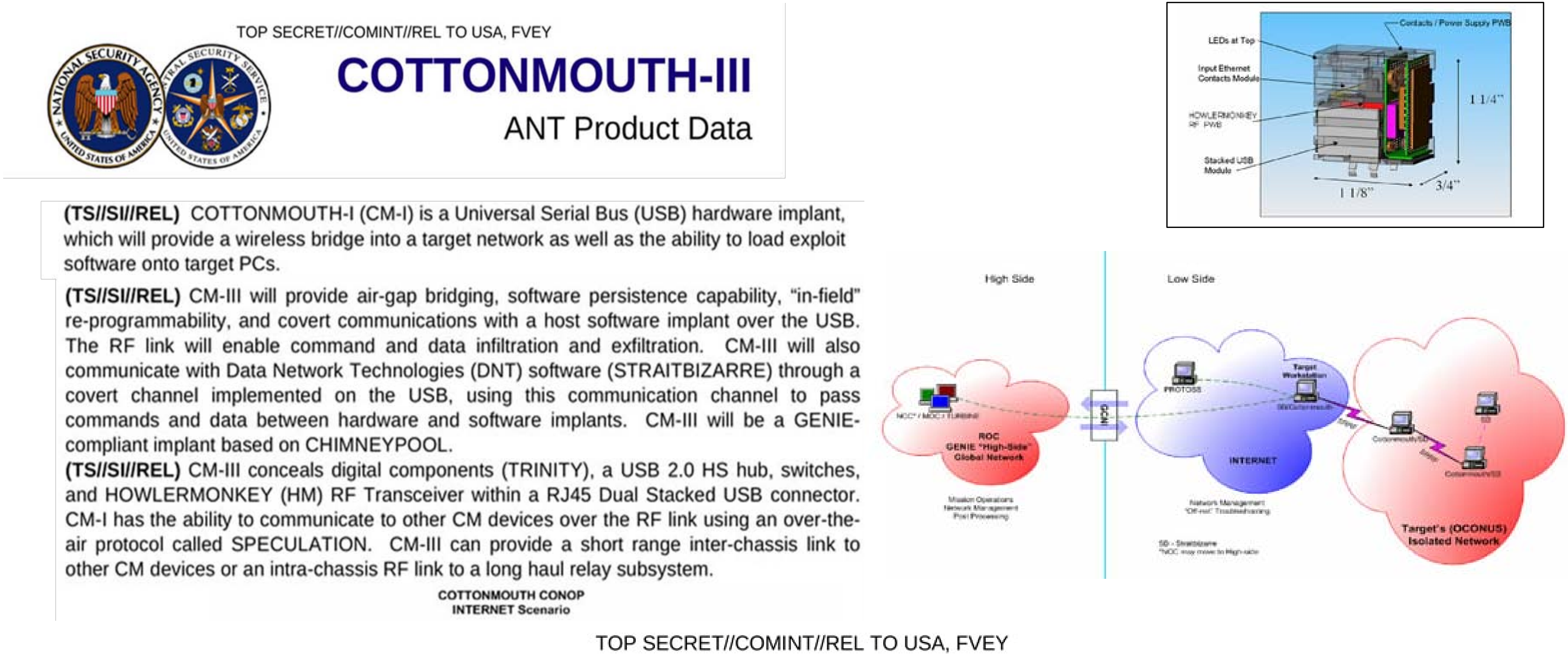
(TS//SI//REL) CM-II will provide software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. CM-II will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-II will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-II consists of the CM-I digital hardware and the long haul relay concealed somewhere within the target chassis. A USB 2.0 HS hub with switches is concealed in a dual stacked USB connector, and the two parts are hard-wired, providing a intra-chassis link. The long haul relay provides the wireless bridge into the target's network.

SB - Straitbizarre
*NCC may move to High-side

TOP SECRET//COMINT//REL TO USA, FVEY

Government Infringement for USB Covert Intelligence Gathering



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-III

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant, which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

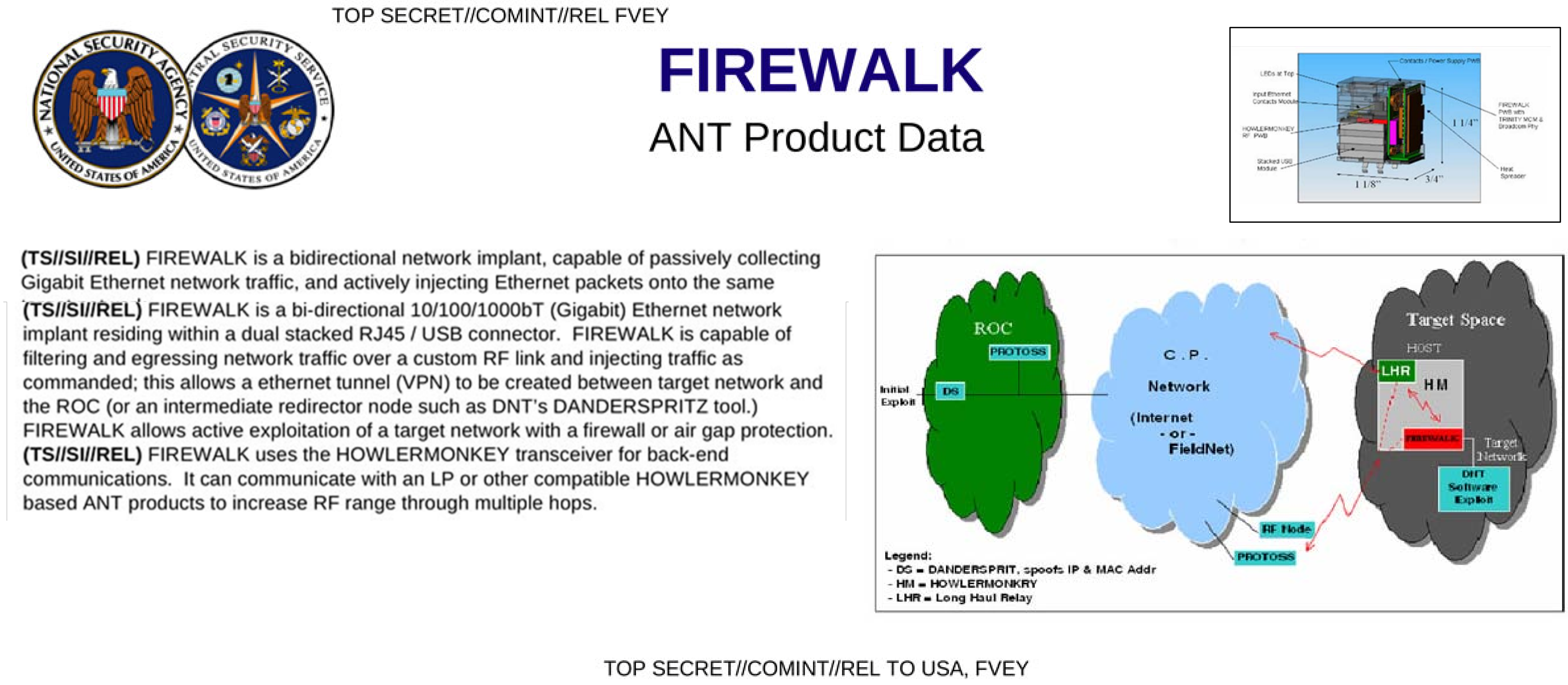
(TS//SI//REL) CM-III will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-III will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-III will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-III conceals digital components (TRINITY), a USB 2.0 HS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within a RJ45 Dual Stacked USB connector. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION. CM-III can provide a short range inter-chassis link to other CM devices or an intra-chassis RF link to a long haul relay subsystem.

COTTONMOUTH CONOP
INTERNET Scenario

TOP SECRET//COMINT//REL TO USA, FVEY

Government Infringement for USB Covert Intelligence Gathering



TOP SECRET//COMINT//REL FVEY

FIREWALK

ANT Product Data

Contacts / Power Supply PWB
LEDs at Top
Input Ethernet Contacts Module
HOWLERMONKEY RF PWB
Stacked USB Module
FIREWALK PWB with TRINITY MCM & Broadcom Phy
Heat Spreader
1 1/4"
1 1/8"
3/4"

(TS//SI//REL) FIREWALK is a bidirectional network implant, capable of passively collecting Gigabit Ethernet network traffic, and actively injecting Ethernet packets onto the same

(TS//SI//REL) FIREWALK is a bi-directional 10/100/1000bT (Gigabit) Ethernet network implant residing within a dual stacked RJ45 / USB connector. FIREWALK is capable of filtering and egressing network traffic over a custom RF link and injecting traffic as commanded; this allows a ethernet tunnel (VPN) to be created between target network and the ROC (or an intermediate redirector node such as DNT's DANDERSPRITZ tool.) FIREWALK allows active exploitation of a target network with a firewall or air gap protection.

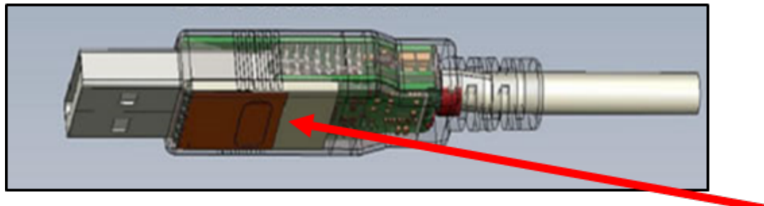
(TS//SI//REL) FIREWALK uses the HOWLERMONKEY transceiver for back-end communications. It can communicate with an LP or other compatible HOWLERMONKEY based ANT products to increase RF range through multiple hops.

TOP SECRET//COMINT//REL TO USA, FVEY

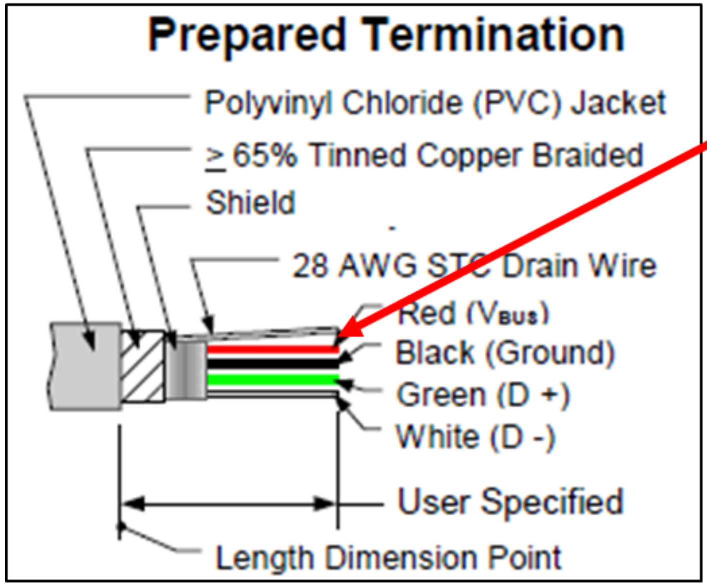
Demodulation Product Description:
Universal Serial Busses (USB)

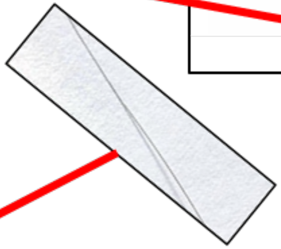
An encoded microwire key is embedded into or onto a miniaturized chip (hardware implant) along with covert software that is inserted into USB devices. The microwire provides a radio frequency link that allows for infiltration and exfiltration of data. The computers or personal electronic devices to which encoded microwire USB keys are attached can be remotely controlled and monitored. The encoded microwire USB keys can also be used to track the location of the attendant device by ISP address at great distances and by microwave interrogation at even greater distances by satellites.

Demodulation Product Description:
Universal Serial Busses (USB)

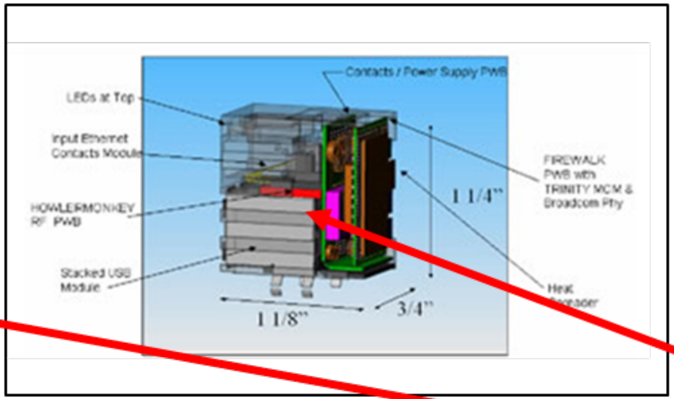


Cottonmouth I





Micorwire



Cottonmouth II

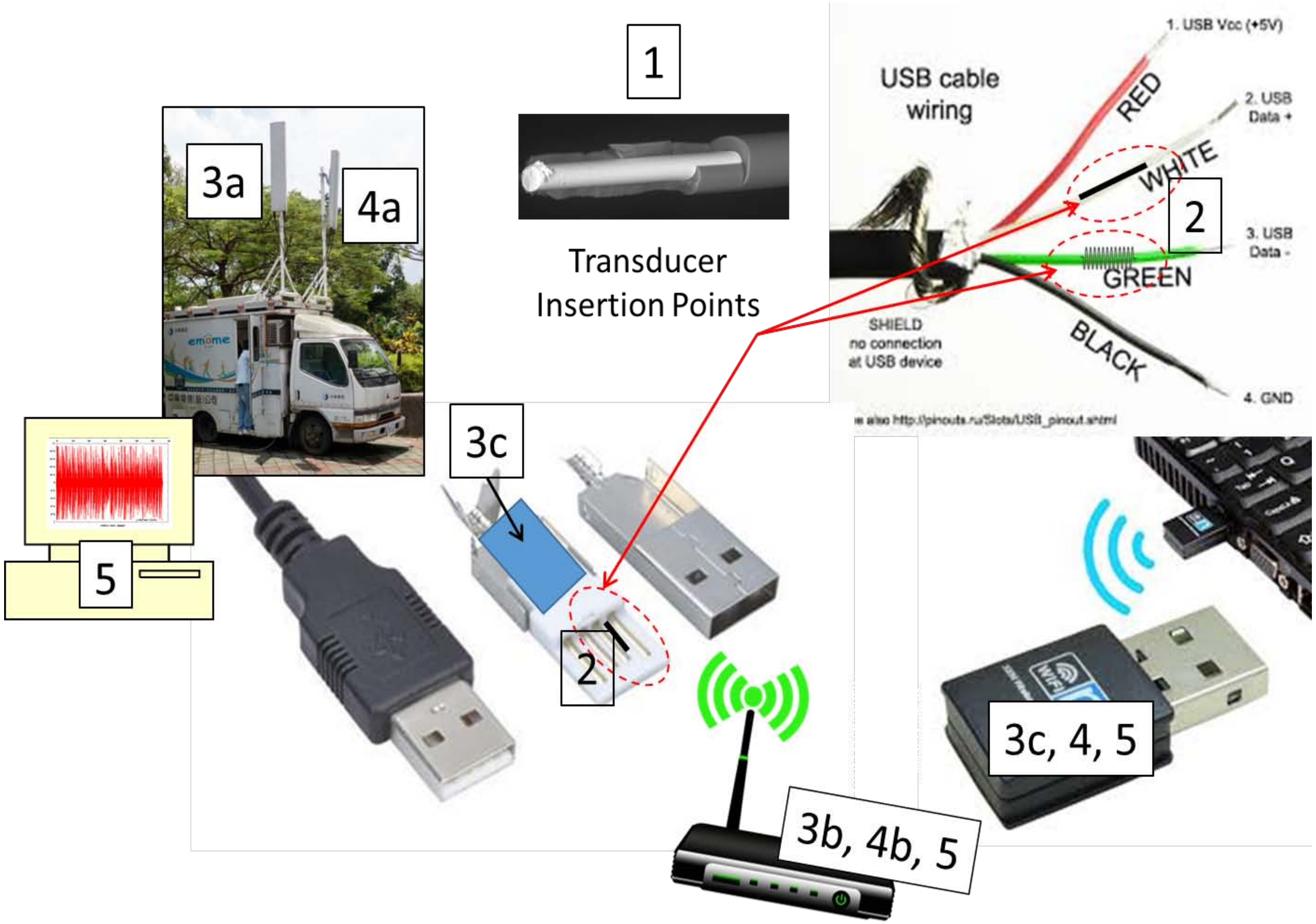
A strand of microwire is laterally embedded along the outside of the red signal carrier line in a USB cable to "read" emanations in real time.

Cottonmouth III

A miniaturized chip embedded with microwire is placed in the USB device

Technical Drawing of Infringement

Component Description/Labeling
1. Magnetic Transducer – Microwire (encoded) inserted into USB plug structure
2. Magnetic modulation – adjacent signal / data modulates microwire transducer
3. Transmitter Source – a. Remote RF System (Tx/Rx or Discrete) b. Co-opted System (e.g. WiFi Router) c. On-board (hardware implant) with USB plug
4. Receiver of Signal – a. Remote RF System (Tx/Rx or Discrete) b. Co-opted System (e.g. WiFi Router)
5. RF Controller, Signal Processing of Return Signal w/Internet Backhaul


1
Transducer Insertion Points
USB cable wiring
1. USB Vcc (+5V)
RED
2. USB Data +
WHITE
2
3. USB Data -
GREEN
SHIELD no connection at USB device
BLACK
4. GND
e also http://pinouts.ru/Slots/USB_pinout.shtml
3a
4a
5
3c
2
3b, 4b, 5
3c, 4, 5